

PUBLICATION

Government Deadline Looms for Training on Insider Threats

Authors: Thomas H. Barnard

May 12, 2017

Almost one year ago, on May 18, 2016, the Department of Defense (DoD) published Change Two to DoD 5220.22-M, the Department of Defense's "National Industrial Security Operating Manual (NISPOM)." This change required all contractors to establish and maintain an insider threat program to detect, deter and mitigate insider threats.

In connection with the NISPOM change, the DoD published Industrial Security Letter 2016-02 (ISL 2016-02), to provide additional information and guidance as to how to comply with the new requirements. While the bulk of the requirements contained therein involved corporate-level programs and policies which were to have been established last year, it also established new training requirements that apply to all employees, including those already cleared and granted access to government information.

What this means to you is that every employee in your organization must complete the required training prior to May 31, 2017, ***even if they already have clearance and have previously been granted access to government information.***

To whom does this apply?

As set forth in ISL 2016-02, "contractor" refers to any industrial, educational, commercial or other entity that has been granted a facility security clearance by a Cognizant Security Agency. As such, the training requirements apply to **all cleared employees of a contractor**, even those employed prior to May 18, 2016.

What are the training requirements?

The training requirements are set forth in NISPOM 3-103a and generally require that all employees are trained to detect and mitigate threats from within their organization that may compromise classified data. This training must be completed by new employees prior to being granted access to classified data and by all employees prior to May 31, 2017. There is also a requirement for annual refresher training.

Where can I find training materials?

The DoD's Defense Security Service (DSS) has made compliant training available through the DSS Center for Development of Security Excellence (CDSE). The courses are located in the CDSE catalog under "Insider Threat." *See Insider Threat Awareness: Course CI121.16 or Counterintelligence Awareness and Security Briefing: Course CI112.16.* These courses are available here:

- <http://www.cdse.edu/catalog/elearning/CI112.html>

What is the consequence if training is not completed on time?

Failure to comply with these new requirements could cause your company to lose its access to classified information, rendering it unable to perform its contractual obligations. It is therefore vital that you ensure all your employees have completed this training by the May 31, 2017 deadline.

If you have any questions or concerns about your organization's data privacy and cybersecurity protocols or industry specific questions, please reach out to Thomas Barnard or any member of Baker Donelson's Data Protection, Privacy and Cybersecurity Group.